

SAFETY INSTRUMENTED SYSTEMS

SAFETY NOTE SN - 5091

TIME - THE MOST IMPORTANT PARAMETER IN SIS FUNCTIONALITY

1. Introduction

When we talk about a Safety Instrumented Systems (SIS) performing its protective action, we use to talk about Probability of Failure on Demand (PFD), Safety Integrity Level (SIL), Risk Reduction Factor (RRF), Programmable Electronics (PE) and non PE Logic Solvers, and use to discuss about diagnostics, redundancy, diversity and architectural constraints. Nobody seems to care about TIME.

And TIME is the most important parameter in SIS functionality, just because all of other parameters depend on it. Let us think about it.

TIME defines the type of SIS we are using, that is a "demand mode" or a "continuous mode" of operation SIS. TIME defines the value of PFD because it depends on Mean Time To Restoration (MTTR) and Proof Time Interval (PTI). RRF decreases while TIME elapses. TIME is critical to the process safety as its Process Safety Time (PST).

But what about the Failure Rate? All components on a SIS can fail. The problem is if that failure will be probable once a year or once in a million years. TIME is what determines it.

So, while SIS is running and trying to protect our lives, the environment and the equipment, TIME is challenging it continuously. This paper is focused to analyze how those action, reaction, intervention and mean times interact while SIS is running.

Our purpose is simply help to prevent conceptual design of the SIS and engineering practices during its design, implementation, maintenance and further changes to be made, not to fail in bringing the SIS the appropriate functional characteristics required for each application to run safely.

First of all, let us state that being a SIS a system composed by three main subsystems, each of them is or could be subjected to the analysis presented on this paper. Hereinafter, then, the word "system" could be applied to a complete SIS or just to one of its subsystems, which are:

- The sensor (input) subsystem, which comprises the actual sensor(s) and any other components (i.e. microprocessors, signal converters, IS barriers, etc.) and its wiring to the logic subsystem.
- The logic subsystem or SIS Logic Solver (SIS-LS), which comprises the component(s) where the signals are first combined, and all other components up to and including where final signal(s) are presented to the final element subsystem
- The final element (output) subsystem, which comprises all the components and wiring which process the final signal(s) from the logic subsystem including the final actuating component(s)

Let's begin then to define the different "TIMES" we will consider in our analysis.

1.1 PTI (Proof Test Interval)

PTI is the elapsed time between two proof tests, being proof test "a periodic test performed to detect failures in a safety-related system so that, if necessary, the system can be restored to an 'as new' condition or as close as practical to this condition"

PTI is the main time to consider, providing it will be determined according to operating conditions of the Equipment Under Control (EUC). Its combination with the Expected Interval Between Demands (EIBD) determines if the system is to be considered as "on demand" or as "continuous mode" type (see Fig. 1 and Fig. 3).

1.2 EIBD (Expected Interval Between Demands)

EIBD is the mean time between two successive demands for the safety function.

This interval is highly dependent of the kind of application the demands could apply to, i.e. EIBD could be very short for probable flame extinction in variable demand boilers, and EIBD could be very long for expected gas leakage in an LPG tank farm. As noted before, its combination with PTI (Proof Test Interval) determines if the system is to be considered as "on demand" or as "continuous mode" type (see Fig. 1 and Fig. 3).

1.3 DTI (Diagnostics Test Interval)

DTI is the interval between two successive diagnostics cycle iterations. It's the "interval between on-line tests to detect faults in a safety-related system that have a specified diagnostic coverage".

DTI is maybe the most important of all of the intervals involved in system safety. The smaller the DTI, the sooner reaction of the system to prevent SIS to fail on its protective action. The smaller the DTI, the smaller Mean Time To Restoration (MTTR) of the system and hence the lower the Probability of Failure on Demand (PFD). DTI must be at least an order of magnitude less than EIBD in "continuous mode" operation (see Fig. 2). Detection Time (DT) will also be improved with little DTI values.

1.4 DT (Detection Time)

DT is the elapsed time between a failure occurring in the system and its detection by the diagnostics subsystem, that is, when the DTI finishes to begin the diagnostics cycle.

1.5 TTS (Time To Safe)

TTS is the time required by the system to bring the EUC to its safe state.

It shall be noted that per IEC 61508 the "safe state" is not defined as a "failsafe" concept (which is usually associated with a simple de-energized state), but a state on which the EUC is not causing harm, accidents, or similar situations, providing it could be either de-energized (i.e. ESD systems), or energized (i.e. F&G systems).

1.6 PST (Process Safety Time)

PST is the period of time between a failure occurring in the EUC or the Basic Process Control System (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety function is not performed.

It is mandatory for the safety system to perform its protective action before the PST elapses.

In order to comply with that, DT and TTS shall be as short as possible to guarantee in no case the total time to perform the safety action be greater than PST (recommended safe value for DT and TTS sum is to be less than or equal to 40% PST).

1.7 MTTR (Mean Time To Restoration)

MTTR is the interval while the system is not providing its protective action because of a system failure. MTTR is not the "mean time to repair the system", which is referred here as MTTRP, but MTTR includes MTTRP and DT among others.

MTTR is part of the PFD calculations and has been standardized by IEC 61508 for PFD sample calculations to 8 hours.

1.7.1 MTTR_D (Mean Time To Restoration for Detected failures)

MTTR_D is the required time to restore system full functionality for detected failures. It includes DT, MTTRP and Time To Safe (TTS) when applicable.

1.7.2 MTTR_U (Mean Time To Restoration for Undetected failures)

MTTR_U is the required time to restore system full functionality for undetected failures. Undetected failures include all failures that cannot be detected by diagnostics subsystem but by proof test. That is the reason because MTTR_U is the sum of the MTTRP and the time remaining, at the moment the failure occurs, up to the end of the PTI.

1.8 MTTRP (Mean Time To RePair)

MTTRP is the actual time required to repair the failure.

As MTTR is established for most calculations in 8 hours, is advisable that MTTRP is not longer than 7 hours, providing a DTI of 1 hour or less is usually implemented, in order to avoid SIL degradation of the system.

2. Case studies

Which follows is the analysis of different cases where "TIMES" mentioned above could play different roles with regards to SIS functionality.

2.1 Fault Tolerant System - On Demand Mode

Let us take a look to Fig. 1. There is represented a time diagram for a "fault tolerant" system working "on demand" mode of operation.

"Fault tolerant" means that the system has some kind of Hardware Fault Tolerance (HFT), that is 1oo2, 1oo2D or 2oo3 voting schemes per IEC 61508 ("quad" systems are not analyzed by IEC).

Being "fault tolerant", the system will also be capable to continue working without EUC protection reduction when a single failure in the safety system occurs.

"Fault tolerant" is the best configuration for a safety system providing it brings the greater on-line time (availability) for the EUC while safety system is always running (compare this to Fig. 4 for a "non fault tolerant" system).

Nevertheless we should be aware about RRF reduction in the 1oo2 architecture, when the system is reduced to 1oo1 during the failure state (when in 1oo1, system becomes less safe because there is just one element to fail in order to produce an accident, while when in 1oo2, it would be required two elements to fail simultaneously, which is much less probable).

Hence failed 1oo2 system shall not be allowed to work for a long time after a single failure occurs unless it has "built-in" comprehensive diagnostics, that is, a 1oo2D system.

Saying "system is working on demand mode" means that PTI is less than, or equal to, two times EIBD, which means that no more than two demands could be expected within the PTI. It shall also be noted that EIBD shall be at least an order of magnitude greater than MTTR (both conditions are established in IEC 61508).

Ricardo A. Vittoni - FSS

Nápoles 3139 - C1431DEA - Cdad. de Buenos Aires - Cel. (11) 15 4416-8977 - ravittoni@gmail.com

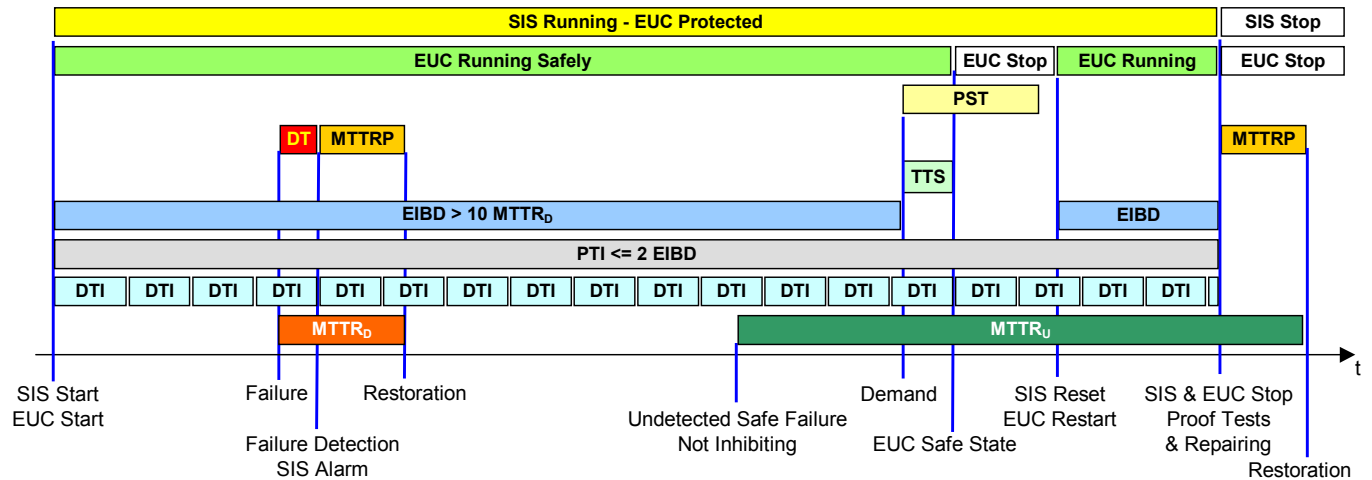


Fig. 1 - On Demand Mode ($PTI \leq 2 * EIBD$) for Fault Tolerant ($HFT > 0$) subsystems - No Dangerous Undetected failures

On the example above, $MTTR_D$ is the sum of DT and $MTTR_P$ and as the system has comprehensive diagnostics (1oo2D and 2oo3 systems), a system alarm is issued to the operator in order to corrective actions can be implemented.

It should be noted that if MTTR was extended for more than 8 hours due to operator inaction or due to problems to get the system repaired, the PFD would be increased and hence RRF would be reduced and its value could be not enough to protect the EUC. This is more critical on 1oo2D systems. That is the reason because some 1oo2D systems has time restriction to operate while 2oo3 system has no time restriction at all.

But what about MTTRU? If time remaining to next proof test is too long the system (working without notice about a failure is present) could become unsafe.

If this is was a non inhibiting failure (i.e. an alarm light not functioning) the system would protect the EUC anyway, when a demand appeared (Fig. 1), but if failure was such that could inhibit the safety system protective action, an accident would occur as shown in Fig. 2.

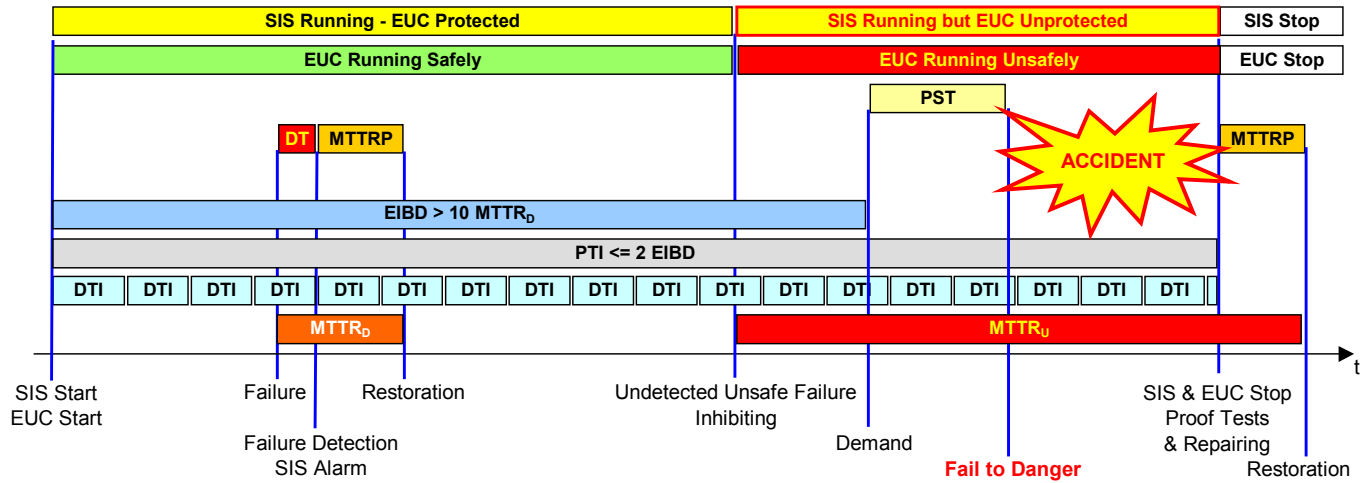


Fig. 2 - On Demand Mode for Fault Tolerant ($HFT > 0$) subsystems - Undetected Dangerous failure

That demonstrates once more the true importance of diagnostics coverage and Safe Failure Fraction (SFF) of the system, providing the less SFF the less probability of a dangerous failure to not be detected and then the less probability of an accident to occur.

An interesting paper written by TUV Rheinland, together with Risknowlogy, explains the differences and the effects diagnostics and proof tests have on the performance of SIS. The paper demonstrates the difference between diagnostic tests and proof tests and what effect they have on the PFD of the safety function. A special performance indicator is used to express this influence and show the effect. The paper can be downloaded from Risknowlogy at <http://www.risknowlogy.com>.

2.2 Fault Tolerant System - Continuous Mode

Let us take a look to Fig. 3. There is represented a time diagram for a "fault tolerant" system working "continuous" mode of operation.

Saying "system is working continuous mode" means that PTI is greater than two times EIBD, which means that more than two demands could be expected within the PTI. It shall also be noted that EIBD

shall be at least an order of magnitude greater than DTI (both conditions are established in IEC 61508).

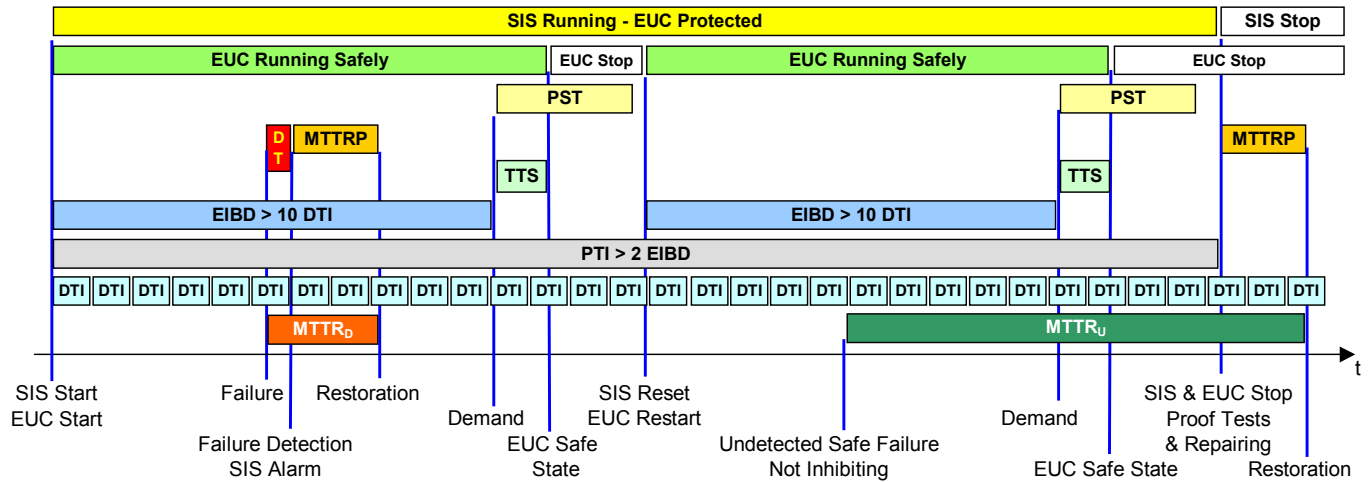


Fig. 3 - Continuous Mode ($PTI > 2 * EIBD$) for Fault Tolerant ($HFT > 0$) subsystems - No Dangerous Undetected failures

Now, in order to avoid misinterpretations in SIS conceptual design and further steps of the Safety Life Cycle (SLC), let us clarify what a "continuous" mode of operation really means.

For example, as stated on our Safety Note SN-5031 related to demonstrate that SIL 3 is required for BMS applications, a BMS should be considered as a "continuous" mode of operation system (although BMS is usually considered as an "on demand" system).

Let us see, how many times a year is expectable to have a trip due to a flame-off demand? Would it be more than twice per year? Sure it is.

And what about PTI? Is it expected to proof the BMS more frequently than once per year in most of the cases? Certainly not.

So, being PTI greater more than twice EIBD, BMS shall be considered as a "continuous" mode SIS according to IEC 61508.

Same case should apply to Critical Control and some ESD applications in the Chemical Industry.

As can be seen in Fig. 3, DT and DTI become more critical on "continuous" mode and then, the equipment shall certainly be of better quality, from the diagnostics safety point of view, than equipment required for "on demand" mode applications.

2.3 Non Fault Tolerant System - On Demand Mode

Let us take a look now to Fig. 4. There is represented a time diagram for a "non fault tolerant" system working "on demand" mode of operation.

Note that "non fault tolerant" does not mean "failsafe" as we mentioned above (see TTS definition).

"Non fault tolerant" means that no Hardware Fault Tolerance (HFT = 0) is available for safety.

In such systems a first failure produces a trip to the "safe state" on the EUC (in "fault tolerant" systems that will happen with the second failure).

It is important to note that for this action is mandatory that the sum of DT and TTS be less than PST (as noted above, a 40% of the PST is advisable). For this reason DTI could be critical.

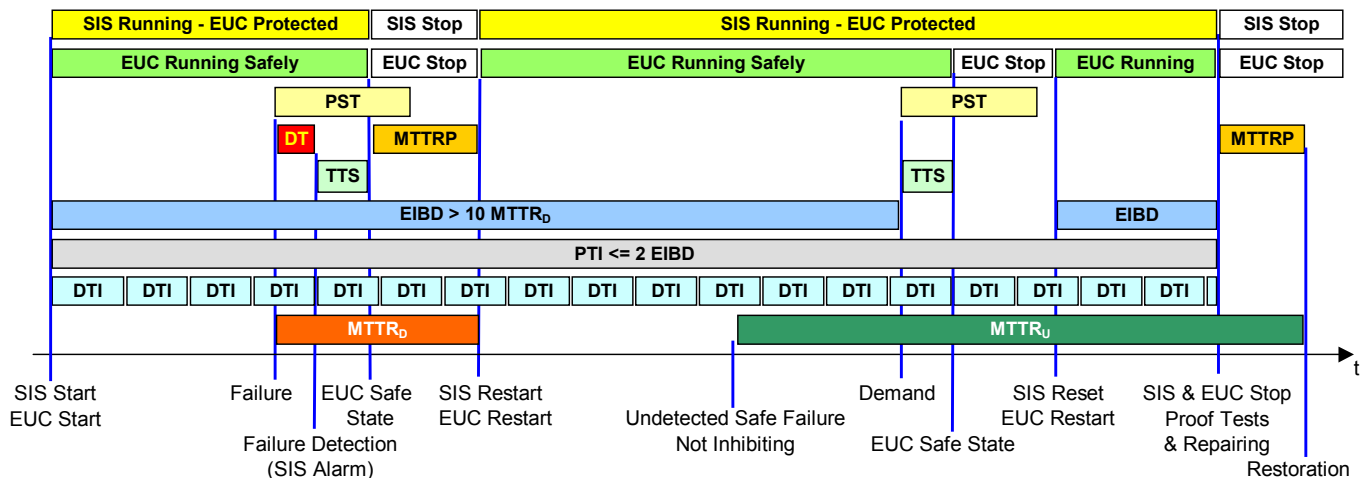


Fig. 4 - On Demand Mode ($PTI \leq 2 * EIBD$) for Non Fault Tolerant ($HFT = 0$) subsystems - No Dangerous Undetected failures

"Non fault tolerant" is not the best configuration for a safety system providing it does not bring the greater on-line time (availability) for the EUC while safety system is not always running (compare this to Fig. 1 for a fault tolerant system).

Ricardo A. Vittoni - FSS

Nápoles 3139 - C1431DEA - Cdad. de Buenos Aires - Cel. (11) 15 4416-8977 - ravittoni@gmail.com

More, a lot of processes have their higher risk level when EUC starts to work and then, stopping and restarting the EUC due to SIS failures, is not a good idea, mainly for continuous processes.

Nevertheless some "on demand" SIS could be "non fault tolerant" providing there is no risk (or risk is acceptable) when SIS stops. Some examples could include F&G alarm and some ESD applications.

3. Conclusions

It has been demonstrated the importance of TIME in different intervals within the SIS functionality. It has also been seen that these "TIMES" can vary from one application to another with different influence in the SIS whole functionality.

Design and Integration Engineers and Technicians shall be aware about the selection of the correct architecture for each system, depending on system application, in way that HFT and diagnostic coverage could reduce the risk and allow more availability to the EUC.

In the same way, the "TIMES" the system will need to handle shall be improved in order to obtain the best performance without sacrificing safety in any case.

Ricardo A. Vittoni - FSS
Functional Safety Specialist